

CLAIMS

What is claimed is:

1. A method of controlling traffic in a computer network, the method comprising:
modifying a data unit to be sent by a first computer, the data unit being intended
5 for a second computer, the data unit being modified such that the data unit is redirected
from the first computer to a third computer;
sending the data unit from the first computer to the third computer; and
forwarding the data unit from the third computer to the second computer.
2. The method of claim 1 wherein the data unit is selected to be modified based on
10 an intended destination of the data unit.
3. The method of claim 1 wherein the data unit is modified in the first computer prior
to initialization of a network-enabled application in the first computer.
4. The method of claim 1 wherein the data unit comprises an Ethernet packet.
5. The method of claim 1 wherein a destination address field of the data unit is
15 modified to contain an address of the third computer in a destination address field and
an address of the second computer in another portion of the packet.
6. The method of claim 1 wherein the second computer comprises a DHCP
(Dynamic Host Configuration Protocol) server.
7. The method of claim 1 further comprising:
20 scanning the data unit for viruses at the third computer.
8. The method of claim 1 wherein the data unit is quarantined at the third computer.

9. The method of claim 1 wherein the third computer is selected to receive the data unit based on an intended destination of the data unit.
10. A system for controlling traffic in a computer network, the system comprising:
a first computer including a kernel driver, the kernel driver being configured to
5 modify a packet generated at the first computer, the packet being intended for a second computer and being modified to be forwarded from the first computer to a third computer.
11. The system of claim 10 wherein the third computer is configured to scan the packet for viruses prior to forwarding the packet from the third computer to the second
10 computer.
12. The system of claim 10 wherein the packet comprises an Ethernet packet.
13. The system of claim 10 wherein the packet is selected to be modified based on the packet's intended destination computer.
14. The system of claim 10 wherein the packet is modified at the first computer prior
15 to initialization of a network-enabled application in the first computer.
15. The system of claim 10 wherein the packet is modified to contain an address of the third computer in a destination address field of the packet and an address of the second computer in another portion of the packet.
16. The system of claim 10 wherein the third computer includes a scanning engine
20 for scanning the packet for viruses.
17. A method of controlling traffic in a computer network, the method comprising:

modifying a DHCP (dynamic host configuration protocol) packet at a first computer prior to initialization of a network-enable application in the first computer, the DHCP packet being intended for a DHCP server, the DHCP packet being modified to be redirected to a second computer;

5 processing the packet at the second computer; and

 forwarding the packet from the second computer to the DHCP server.

18. The method of claim 17 wherein processing the packet at the second computer includes scanning the packet for viruses.

19. The method of claim 17 wherein modifying the packet at the first computer
10 comprises including an address of the second computer in a destination address field of the packet and including an address of the DHCP server in another portion of the packet.

20. The method of claim 17 further comprising:

 forwarding a response packet from the DHCP server to the first computer after
15 the packet is forwarded from the second computer to the DHCP server.